

**REMARKS**

This Application has been carefully reviewed in light of the Office Action mailed June 7, 2006 (the "Office Action"). At the time of the Office Action, Claims 1-30 were pending in the Application. Claims 1-30 were rejected. Applicant respectfully requests reconsideration and favorable action in this case.

**Section 102 Rejections**

Claims 1, 12, 18, 23, and 28 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,275,941 issued to Saito et al. ("*Saito*"). Applicant respectfully traverses these rejections for the reasons stated below.

In order to establish a *prima facie* case of anticipation, all the elements of the claimed invention must be found within a single prior art reference. *Dewey & Almy Chemical Co. v. Mimex*, 124 F.2d 986, 52 USPQ 138 (2d Cir. 1942). Applicant respectfully submits that each and every element of Claims 1, 12, 18, 23, and 28 is not found within the *Saito* reference.

Claim 1 recites:

A method for authenticating and authorizing a user of an electronic device in communication with a network, comprising:

receiving a user request from a user of an electronic device in communication with a network;

searching for information relating to said user in a repository of user information, said searching based at least partially on said user request and a login identity supplied by said user;

retrieving, from the repository of user information, a unique universal user identifier representing said user upon locating said information of said user;

storing at least said unique universal user identifier in a data packet;

sending said data packet to a storage device such that said data packet is transmittable to electronic devices in communication with said network when said user attempts to access a resource within said network; and

retrieving an authorization datum associated with said user, based at least partially on said unique universal user identifier, from said resource.

Applicant submits that *Saito* fails to teach, suggest, or disclose each of these elements. For example, *Saito* fails to teach, suggest, or disclose “searching for information relating to [a] user in a repository of user information . . . based at least partially on [a] user request and a login identity supplied by said user” and “retrieving . . . a unique universal user identifier representing said user upon locating said information of said user.” Instead, *Saito* discloses an integrated authentication server that receives an integrated certificate corresponding to a user and then retrieves authentication information, such as a user ID and password, for the user. *See* abstract; col. 5, ll. 33-50; col. 6, l. 59 - col. 7, l. 4. However, searching based on an integrated certificate is not the same as “searching based at least partially on [a] user request and a login identity supplied by [the] user.” Moreover, retrieving authentication information such as user ID and password is not the same thing as “retrieving . . . a unique universal user identifier.” For at least these reasons, the rejection of Claim 1 is improper.

In response, the Examiner cites col. 2, ll. 28-39 and col. 5, ll. 51-56 of *Saito*. *See* Response to Arguments, Office Action, p. 2. However, these portions of *Saito* fail to teach, suggest, or disclose “retrieving . . . a unique universal identifier . . . upon locating said information of said user.” Instead, the portions of *Saito* cited by the Examiner disclose generating -- not retrieving -- an integrated certificate. *See* col. 5, ll. 51-56 (“For a user who has no integrated certificate, an integrated certificate is *issued* through the conventional log-in effected by inputting a user ID and a password . . .” (emphasis added)); col. 2, ll. 28-39 (“the integrated authentication server may check the user for the right to access the application server and if valid, the integrated authentication server may *prepare* a temporal integrated certificate . . .” (emphasis added)). As such, the arguments advanced by the Examiner are misdirected. None of the portions of *Saito* cited by the Examiner -- in either his claim rejection or his Response to Arguments -- teach, suggest, or disclose “searching for information relating to [a] user in a repository of user information . . . based at least partially on [a] user request and a login identity supplied by said user” and “retrieving . . . a unique universal user identifier representing said user upon locating said information of said user.” For at least this reason, the rejection of Claim 1 is improper. Therefore, Applicant respectfully requests that the rejection of Claim 1 be withdrawn.

Claims 12, 18, 23, and 28 include limitations similar to those in Claim 1. For example, Claim 12 recites “providing identifying data to said network” and “retrieving, in response to the identifying data, a unique universal user identifier corresponding to said user

from a repository of unique universal user identifier.” Similarly, Claim 18 recites “accessing a repository containing a plurality of unique universal user identifiers, each of said unique universal user identifiers being unique to a user” and “retrieving one of said unique universal user identifiers from said repository.” Claim 23 recites “a first software tool operable to receive user login information, access said repository” and “retrieve a unique universal user identifier relating to said user.” Likewise, Claim 28 recites “searching for a user credential corresponding to said user in an authentication database,” “locating said user credential in said authentication database,” and “retrieving a unique universal user identifier representing said user upon locating said user credential.” Therefore, Applicant submits that Claims 12, 18, 23, and 28 are allowable, for example, for reasons similar to those discussed above with regard to Claim 1. As such, Applicant respectfully requests that the rejection of Claims 12, 18, 23, and 28 be withdrawn.

### **Section 103 Rejections**

Claims 12-16 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,178,511 issued to Cohen et al. (“*Cohen*”) in view of U.S. Patent No. 6,609,198 issued to Wood et al. (“*Wood*”) and also in view of U.S. Patent No. 6,898,577 issued to Johnson (“*Johnson*”). Applicant respectfully traverses these rejections for the reasons stated below.

In order to establish a *prima facie* case of obviousness of a claimed invention, all claim limitations must be taught or proposed by the prior art. *In re Royka*, 490 F.2d 981 (CCPA 1974). Applicant respectfully submits that each and every element of Claims 12-16 is not found within the references cited by the Examiner.

Claim 12 recites:

A method for accessing a plurality of resources having different authorization requirements, comprising:  
accessing, via an electronic device, a network comprising a plurality of resources;  
providing identifying data to said network;  
retrieving, in response to the identifying data, a unique universal user identifier corresponding to said user from a repository of unique universal user identifiers;  
storing said unique universal user identifier on a storage device, said unique universal user identifier indicating said user is authenticated; and

accessing one of said plurality of resources, wherein said unique universal user identifier is transmitted to said one of said plurality of resources to identify said user such that said user can access authorized resources without providing additional identifying information and said user is denied access to unauthorized resources.

Applicant submits that the *Cohen-Wood-Johnson* combination suggested by the Examiner fails to teach, suggest, or disclose each of these elements. For example, the *Cohen-Wood-Johnson* combination fails to teach, suggest, or disclose “retrieving . . . a unique universal user identifier corresponding to said user.” Instead, the portion of *Wood* relied upon by the Examiner discloses “associating a unique session identifier with a set of access requests originating from a client entity and maintaining the unique session identifier across a credential level change.” Col. 3, ll. 4-6 (emphasis added). A session identifier, however, is not a unique universal user identifier. As defined by *Wood*, a session is a “period and collection of states spanning one or more interactions between an entity [e.g., user] and an information environment.” Col. 5, ll. 25-36; *see also* col. 5, ll. 15-24. Since this definition distinguishes between a user and a session, the two cannot be analogous. Because of this, *Wood*’s session identifier also cannot be a unique universal user identifier. Moreover, since a user in *Wood* could have multiple sessions with multiple information environments, the user in *Wood* could have multiple unique session identifiers. As such, *Wood*’s unique session identifier is hardly a unique universal user identifier. Therefore, *Wood* clearly fails to teach, suggest, or disclose a unique universal user identifier as recited in Claim 12. For at least this reason, the rejection of Claim 12 is improper. As such, Applicant respectfully requests that the rejection of Claim 12 be withdrawn.

Claims 13-16 depend from Claim 12. Therefore, Applicant submits that Claims 13-16 are allowable, for example, for reasons similar to those discussed above with regard to Claim 12. As such, Applicant respectfully requests that the rejection of Claims 13-16 be withdrawn.

Claims 1-4, 6-11, and 18-30 were rejected under U.S.C. § 103(a) as being unpatentable over *Cohen* in view of U.S. Publication No. 2002/0161901 for Weissman (“*Weissman*”) and also in view of *Wood* and *Johnson*. Applicant respectfully traverses these rejections for the reasons stated below.

Claim 1 recites:

A method for authenticating and authorizing a user of an electronic device in communication with a network, comprising:

receiving a user request from a user of an electronic device in communication with a network;

searching for information relating to said user in a repository of user information, said searching based at least partially on said user request and a login identity supplied by said user;

retrieving, from the repository of user information, a unique universal user identifier representing said user upon locating said information of said user;

storing at least said unique universal user identifier in a data packet;

sending said data packet to a storage device such that said data packet is transmittable to electronic devices in communication with said network when said user attempts to access a resource within said network; and

retrieving an authorization datum associated with said user, based at least partially on said unique universal user identifier, from said resource.

Applicant submits that the *Cohen-Weissman-Wood-Johnson* combination suggest by the Examiner fails to teach, suggest, or disclose each of these limitations. For example, the *Cohen-Weissman-Wood-Johnson* combination fails to teach, suggest, or disclose “retrieving, from the repository of user information, a unique universal user identifier representing said user.” Instead, as mentioned above with regard to Claim 12, the portion of *Wood* relied upon by the Examiner discloses “associating a unique session identifier with a set of access requests originating from a client entity and maintaining the unique session identifier across a credential level change.” Col. 3, ll. 4-6 (emphasis added). A session identifier, however, is not a unique universal user identifier. Therefore, for at least this reason, the rejection of Claim 1 is improper. As such, Applicant respectfully requests that the rejection of Claim 1 be withdrawn.

Claims 18, 23, and 28 recite limitations similar to those in Claim 1. For example, Claim 18 recites “accessing a repository containing a plurality of unique universal user identifiers, each of said unique universal user identifiers being unique to a user” and “retrieving one of said unique universal user identifiers from said repository.” Similarly, Claim 23 recites “a first software tool operable to receive user login information, access said repository” and “retrieve a unique universal user identifier relating to said user.” Likewise,

Claim 28 recites “searching for a user credential corresponding to said user in an authentication database,” “locating said user credential in said authentication database,” and “retrieving a unique universal user identifier representing said user upon locating said user credential.” Therefore, Applicant submits that Claims 18, 23, and 28 are allowable, for example, for reasons similar to those discussed above with regard to Claim 1. As such, Applicant respectfully requests that the rejection of Claims 18, 23, and 28 be withdrawn.


Claims 2-4, 6-11, 19-22, 24-27, 29 and 30 depend from Claims 1, 18, 23, and 28. Therefore, Applicant submits that Claims 2-4, 6-11, 19-22, 24-27, 29 and 30 are allowable, for example, for reasons similar to those discussed above with regard to Claims 1, 18, 23, and 28. As such, Applicant respectfully requests that the rejection of Claims 2-4, 6-11, 19-22, 24-27, 29 and 30 be withdrawn.

**CONCLUSION**

Applicant has made an earnest attempt to place this case in condition for allowance. For the foregoing reasons, and for other apparent reasons, Applicant respectfully requests full allowance of all pending Claims. If the Examiner feels that a telephone conference would advance prosecution of this Application in any manner, the undersigned attorney for Applicant stands ready to conduct such a conference at the convenience of the Examiner.

Applicant believes no fee is due. However, should there be a fee discrepancy, the Commissioner is hereby authorized to charge any required fees or credit any overpayments to Deposit Account No. 02-0384 of Baker Botts L.L.P.

Respectfully submitted,  
BAKER BOTTS L.L.P.  
Attorneys for Applicant



Matthew A. Hayenga  
Reg. No. 54,156  
Phone: (214) 953-6747

Date: July 24, 2006

**CORRESPONDENCE ADDRESS:**

Customer Number: **05073**  
Attorney Docket No.: 063170.6963